

March 10, 1999

Shirley Ann Jackson
Chairman
Nuclear Regulatory Commission
Washington, DC 20555

Dear Ms. Jackson:

I am writing in regard to the Nuclear Regulatory Commission's (NRC's) oversight of nuclear plants' response to the "Y2K" bug. In light of the possibility that the Y2K bug may threaten the safe operation of nuclear plants in this country and throughout the world, I urge you to consider more aggressive action to forestall any Y2K problems and to deal effectively with any problems that occur.

As you know, particularly in the early years of computer programming, many computer programs were written to handle only the last two digits of the year. Such programs may crash or may give unexpected results when given a date in the year 2000 or later. This so-called "Y2K bug" is particularly common in programs from the 1970's, when most U.S. nuclear plants were being built. Thus an NRC audit last fall of one plant, Seabrook in New Hampshire, found 1304 "software items and embedded systems potentially affected by the Y2K problem." 12 items were determined to have "safety implications," 18 others could cause a plant trip (sudden shutdown) or reduction of generated power, and an additional 159 are computer programs or embedded systems that are required by NRC regulations. Of the 1304 items, Seabrook intends to fix, replace, or eliminate 532 items, and considers the rest Y2K compliant or acceptable without further testing or action.

The NRC continues to maintain that, as stated on its WWW page "Y2K and Nuclear Reactors" (<http://www.nrc.gov/NRC/Y2K/Y2KNRR.html>), "The NRC has no indication that significant Y2K problems exist with safety-related systems in nuclear power plants for those systems that directly affect the ability to safely operate and shut down the plants." Some nuclear safety experts, however, have suggested that Y2K bugs in systems that are not technically needed to shut down a nuclear plant could nonetheless cause safety problems. For example, Y2K bugs in plant monitoring computers, such as those that were crashed by Y2K testing at the Peach Bottom plant in Pennsylvania on February 8, 1999, could force plant operators to rely on unfamiliar analog systems; in effect, computer failure could lead to human failure. Moreover, Y2K bugs in plant security computers could compromise plants' ability to repel outside attacks or could hinder access by needed plant personnel.

In addition, Y2K problems in electricity grids that provide outside power would force plant shutdowns and force plants to rely on backup diesel generators to keep coolant flowing around the fuel rods in the reactor and in the spent fuel pools. At least 46 generator problems were reported by NRC licensees in 1997-1998. At the Pilgrim plant in Massachusetts, for example, the temperature in the generator room dipped below the design minimum twice, the temperature exceeded the design maximum once, a review determined that a single failure of a valve could prevent operation of the generators, and the Technical Specification minimum capacity for the diesel oil tanks was found not to be large enough to handle possible accidents.

I am pleased that the NRC has taken steps to increase its licensees' awareness of the Y2K issue. The May 11, 1998 NRC Generic Letter 98-01 requested that plants certify if they are "Y2K ready" by July 1, 1999, and the January 14, 1999 Supplement 1 to the letter suggested that plants voluntarily include systems that are not "safety-related," many of which can in fact have safety implications. In addition, I understand that the NRC is conducting detailed audits at 12 selected plants and has announced its

intention to have resident inspectors inspect Y2K readiness at all other commercial nuclear plants. I commend the NRC for taking these actions.

However, I am concerned that additional steps may be needed to ensure that all nuclear utilities adequately address Y2K problems before the impending—and fixed—millennial deadline. For this reason, I hope the Commission will consider the following suggestions for additional NRC actions:

1. Require additional licensee testing, reporting, and auditing. Y2K bugs in "embedded systems" can be difficult to identify, and vendor certification is unreliable (see, for example, the audit report from the Hope Creek plant in New Jersey). Companies frequently underestimate the time and effort necessary to fix Y2K problems, but the deadline cannot be moved. Therefore, I urge the NRC to require licensees to inventory all Y2K susceptible systems, rigorously to test necessary computer systems for Y2K compliance, and to report at least bimonthly on progress toward Y2K compliance for each system. In addition, independent audits by Y2K experts at all plants are necessary to ensure that plants are considering all relevant systems. The General Accounting Office made similar recommendations in a March 6, 1998 letter from Dr. Rona B. Stillman, Chief Scientist for Computers and Telecommunications to David Meyer, Chief of the Rules and Directives Branch of the NRC Division of Administrative Services.
2. Require adequate backup electricity systems. The NRC has identified station blackout as one of the most likely causes of a core damage accident. The combination of the likelihood of grid failures due to Y2K bugs and frequent problems with backup diesel generators at nuclear plants heightens the risk of station blackout at the turn of the year. The NRC should include backup diesel generator reliability in Y2K inspections and in periodic Y2K reports, require all licensees to have *all* backup electricity sources available at the turn of the year and other key Y2K dates, and ensure adequate fuel supply.
3. Shut down unsafe plants. The NRC Draft Contingency Plan for the Year 2000 Issue in the Nuclear Industry suggests that the NRC may allow plants to violate their licenses in order to keep the plants producing electricity "in the best interest of maintaining public health and safety during the Y2K transition period." NRC's mandate is to ensure that nuclear plants are operated safely; the reliability of the electrical grid is the responsibility of the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Council (NERC), and state Public Utility Commissions (PUC's). Public health and safety demands that plants that have Y2K bugs in key systems be shut down, before the new year if known in advance, and during the transition if necessary.
4. Assist Russia and other nations with severe Y2K problems. Chernobyl showed that nuclear accidents do not recognize national boundaries. I understand that the NRC is currently providing some technical assistance to foreign nations in addressing Y2K issues at their reactors, but I am concerned that sufficient resources may not be available for this purpose. I urge you to secure additional funding to ensure that Russia and other nations, many of which are far behind the U.S. in facing nuclear Y2K issues, are able to resolve safety-related Y2K problems.

In addition, I request your assistance in answering the following questions regarding Y2K problems at commercial nuclear power plants:

1. The NRC's Generic Letter 98-01 defines "Y2K ready" as "determined to be suitable for continued use into the year 2000 even though the computer system or application is not fully Y2K compliant." The GAO letter mentioned above notes that "This determination involves making judgments about suitability. The proposed generic letter does not require the licensees to state how and why they determined that a non-compliant system would be suitable for continued use." How will the NRC evaluate a licensee claim to be Y2K ready without a clear definition, detailed description, or actual testing?

2. The Y2K audit of the Seabrook plant noted that the vendor will not make the required "Radiation Data Monitor System" Y2K compliant, and that the vendor recommends setting the computer clock back to another year, such as 1972. Is this a common method of making systems "Y2K ready," and is it considered an acceptable long-term solution?
3. In light of the ongoing problems with the backup diesel generators at the Pilgrim plant, what are the NRC and the Pilgrim plant doing to ensure that multiple backup electricity sources and adequate fuel are available in case of Y2K related problems at the site or in the Northeastern electricity grid?
4. Does the NRC consider reliance upon vendors to certify the Y2K compliance of their own systems to be an adequate response for Y2K susceptible required plant systems?
5. Will the Y2K inspections conducted by resident NRC inspectors require complete inventories of Y2K susceptible software and embedded systems, justification of licensee claims of Y2K readiness, and rigorous testing of Y2K compliance in systems required by regulation? The the Pilgrim plant, for example, according to a Boston Edison spokesman in a March 9, 1999 article in the *Boston Herald*, "will be finished with its millennium computer bug fix in about three months." Will Pilgrim receive as exacting a Y2K audit as its neighbor Seabrook in order to confirm this claim? Will the NRC inspectors provide ongoing monitoring of progress toward full Y2K compliance at all plants? What criteria will the NRC use for requiring nuclear plant shutdowns or other action in the case of failure to achieve necessary Y2K readiness before the end of the year?
6. Why does NRC believe there is a "public health and safety" need to keep nuclear plants running during the Y2K transition? Has the NRC been informed by FERC or NERC that keeping particular nuclear plants running is necessary in order to prevent grid shutdowns? If so, please provide written documentation. Under what conditions would nuclear plants be allowed to operate outside license conditions and for how long?

Thank you for your assistance. If you have questions concerning this letter please feel free to contact Mr. Lowell Ungar or Mr. Jeffrey Duncan on my staff at (202)225-2836.

Sincerely,

Edward J. Markey
Member of Congress